What is claimed is:

1. A wide area network using the internet as a backbone, comprising:

a first dedicated line coupled to a first participating ISX/ISP provider of internet access;

a source router having a channel service unit having an output coupled to said first dedicated line;

a source firewall circuit having a first port for coupling directly or through a local area network to a first device for which communication over said wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encrypt the payloads of downstream WAN packets being transmitted via the WAN interface to said source router using any encryption method having a user definable key or keys, and for decrypting the payloads of any incoming upstream WAN packets arriving from said source router via said WAN interface using the same encryption method and user definable key or keys that were used to encrypt the outgoing WAN packets;

one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers functioning to implement a predetermined private tunnel data path coupling a router of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider through said routers of said participating ISX/ISP providers;

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated line to said router of said endpoint ISX/ISP provider;

a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a device for which communication across said wide area network is desired, said firewall functioning to encrypt the payloads of upstream WAN packets being transmitted through said WAN interface to said destination router for transmission to said source router via said private tunnel using the same encryption method used by said source firewall and the

same user definable key or keys used by said source firewall circuit, and for decrypting any incoming packets from said source router arriving from said endpoint participating ISX/ISP provider using the same encryption protocol used by said source firewall and the same user definable key or keys used by said source firewall circuit and transmitting the decrypted packets to said second device.

2. A process for launching downstream AlterWAN packets addressed to an AlterWAN destination into a private tunnel coupling two AlterWAN destinations using the internet as a backbone and for launching non-AlterWAN packets into a normal internet traffic routing data path, comprising the steps:

receiving at a source firewall an incoming downstream wide area network packet from a workstation or other device at a first customer location said incoming downstream wide area network packet being either addressed to an AlterWAN destination or not an AlterWAN packet;

at said source firewall, using the destination address in said incoming downstream wide area network packet to determine if said packet is addressed to an AlterWAN destination coupled to said source firewall by a private tunnel using the internet as a backbone (hereafter referred to as an AlterWAN packet) or is addressed to some non-AlterWAN website or location on the internet (hereafter referred to as a non-AlterWAN packet);

if said packet is an AlterWAN packet, encrypting at said source firewall the payload portion thereof and forwarding the encrypted AlterWAN packet to a source router;

if said packet is a non-AlterWAN packet, at said source firewall, forwarding said non-AlterWAN packet to said source router without encrypting the payload portion thereof;

at said source router, converting both said AlterWAN packets and said non-AlterWAN packets into signals suitable for transmission on a dedicated telephone line or other transmission medium coupling said source router to a specially selected first ISX/ISP provider and transmitting said signals to said specially selected ISX/ISP provider, said specially selected ISX/ISP provider being selected either because their routing tables are such that AlterWAN packets will naturally be routed

along high bandwidth, low hop-count data paths to the next ISX/ISP provider in said virtual private network or because the routing tables of the router of said first ISX/ISP provider have been altered to insure that AlterWAN packets get routed along high bandwidth, low hop-count data paths to the next ISX/ISP provider along said private tunnel.

3. An apparatus comprising:

a dedicated data path for coupling to a specially selected first participating ISX/ISP provider of internet access;

a firewall circuit having a first port for coupling directly or through a local area network to one or more devices for which communication over a wide area network using the internet as a backbone is desired, and having a second port, said firewall functioning to to use the destination addresses in the headers of each packet received from said one or more devices to distinguish between AlterWAN packets which are packets addressed to destination devices coupled to said firewall circuit via a private tunnel through the internet, and conventional packets which are packets not addressed to destination devices coupled to said firewall circuit via a private tunnel through the internet, said firewall circuit functioning to encrypt the payloads of outgoing AlterWAN packets using one or more predetermined keys and an encryption algorithem, and sending said encrypted AlterWAN packets to said source router via said second port, and functioning to forward any conventional packets to said source router, and functioning to decrypt any incoming AlterWAN packets arriving from said source router using the the same encryption algorithms and one or more predetermined keys which were used to encrypt the packets at the location from which they were sent;

a source router having an input coupled to said second port of said firewall circuit either directly or by a local area network connection, and having a channel service unit having an output coupled to said dedicated data path, said channel service unit functioning to convert digital data packets received from said firewall circuit into signals suitable for transmission over whatever type of transmission medium is selected for said dedicated data path, and for converting signals received from said dedicated data path into data packets, said source router for transmitting both

AlterWAN and non-AlterWAN packets over said dedicated data path to said specially selected first participating ISX/ISP provider where AlterWAN packets will be routed via said private tunnel and specially seleted ISX/ISP providers to their destination and non-AlterWAN packets will be routed along paths on the internet other than said private tunnel.

4. A method of designing and implementing a wide area network using the internet as a backbone, comprising the steps:

1) selecting source and destination sites that have devices that need to be connected by a wide area network;

2) examining the ISX/ISP internet service providers that exist between said source and destination sites and selecting two or more of such ISX/ISP providers through which data passing between said source and destination sites will be routed, said selection being based upon how many hops the routers at those sites will cause packets travelling between said source and destination sites to take and whether the average available bandwidth of the data paths along which the packets travelling between said source and destination sites will travel is substantially greater than the worst case bandwidth consumption of traffic between said source and destination sites;

3) coupling a source firewall to the devices at said source site and configuring said firewall to examine the destination addresses of packets received from said devices at said source site and encapsulate each packet addressed to any device at said destination site in an internet protocol packet, hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the address of an untrusted port of a destination firewall at said destination site and having the original IP packet as its payload, said source firewall being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any packets received from said devices at said source site which are not addressed to any device at said destination site, and configuring said source firewall to recognize any incoming AlterWAN packets which have as their destination addresses the IP address of the untrusted side of said source firewall and

to strip off the AlterWAN packet headers and decrypt the payload portion of each said AlterWAN packet to recover the original IP packet transmitted from said destination site using the same encryption algorithm and the same encryption key or keys used to encrypt the payload portions of said AlterWAN packets at said destination site and for outputting said recovered the original IP packet to said devices at said source site, said source firewall having an untrusted port;

4) coupling a source router to receive said encrypted and non-encrypted packets from said untrusted port of said source firewall and to convert them in a channel service unit to signals suitable for transmission over a first dedicated local loop connection;

5) contracting to establish said first dedicated local loop connection between the output of said source router at which said signals appear and a first participating ISX/ISP provider in the group of ISX/ISP providers selected in step 2;

6) providing a destination router at said destination site having a channel service unit which functions to receive from a second dedicated local loop connection downstream signals encoding both encrypted AlterWAN packet and conventional IP packets and converting said signals back into the original digital packet form and outputting the recovered downstream packets at a firewall port, and said destination router configured to receive upstream AlterWAN and conventional packets and convert them into signals suitable for transmission on said second dedicated data path coupling said destination router to an endpoint participating ISX/ISP provider in the group of ISX/ISP providers selected in step 2 and transmitting said signals on said second dedicated local loop connection;

7) contracting to provide a second dedicated local loop connection connecting the input of said destination router to said endpoint participating ISX/ISP provider, said second dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume;

8) providing a destination firewall having an untrusted port having an IP address coupled to said firewall port of said destination router to receive said recovered digital packets, and configuring said destination firewall to recognize as AlterWAN packets incoming recovered packets having as their destination address the IP address of said destination firewall untrusted input port and to strip off the

AlterWAN packet header and decrypt the payload portion of said AlterWAN packet using the same encryption algorithm and encryption key or keys that were used to encrypt the packet at said source firewall, and configuring said destination firewall to output the decrypted packets at an output coupled to devices at said destination site, and configuring said destination firewall to examine the destination addresses of upstream IP packets received from said devices at said destination site and encapsulate each upstream IP packet addressed to any device at said source site in another IP packet, hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the IP address of an untrusted port of said source firewall at said source site and having the original IP packet as its payload, said destination firewall being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any IP packets received from said devices at said destination site which are not addressed to any device at said source site (hereafter referred to as conventional packets), and said destination firewall configured to transmit said encrypted AlterWAN packets and said conventional packets to said destination router via said untrusted port.

5. A wide area network using the internet as a backbone, comprising:

a first dedicated line coupled to a first participating ISX/ISP provider of internet access;

a source router having a channel service unit having an output coupled to said first dedicated line;

a source firewall circuit having a first port for coupling directly or through a local area network to a first device for which communication over said wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encrypt the payloads of downstream WAN packets being transmitted via the WAN interface to said source router using a first encryption method having a first set of user definable keys which may be only one key, and for decrypting the payloads of any incoming upstream WAN packets arriving from said first participating ISX/ISP using a second encryption method which is different than said

first encryption method and a second set of user definable keys which are different than the first set of user definable keys were used to encrypt the downstream WAN packets;

one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers functioning to implement a predetermined private tunnel data path coupling a router of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider through said routers of said participating ISX/ISP providers;

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated line to said router of said endpoint ISX/ISP provider;

a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a device for which communication across said wide area network is desired, said destination firewall functioning to encrypt the payloads of upstream WAN packets being transmitted through said WAN interface to said destination router for transmission to said source router via said private tunnel using the same encryption method and user definable key or keys used by said source firewall to decrypt upstream WAN packets, and for decrypting any incoming downstream WAN packets from said source router arriving from said destination router via the router of said endpoint participating ISX/ISP provider using the same encryption method and encryption key or keys used by said source firewall to encrypt downstream WAN packets and transmitting the decrypted packets to said second device.